

**Hazard Analysis Procedure**

**for**

**Hazard Category 2 and 3 Nuclear Facilities**

**Revision 1**

**September 2002**

*University of California*



## CONTENTS

---

	<u>Page</u>
1.0 PURPOSE.....	1-1
2.0 SCOPE .....	2-1
2.1 INPUTS .....	2-1
2.2 OUTPUTS.....	2-1
3.0 TERMS AND DEFINITIONS.....	3-1
4.0 RESPONSIBILITIES .....	4-1
4.1 FACILITY MANAGER .....	4-1
4.2 DOCUMENTED SAFETY ANALYSIS LEADER.....	4-1
4.3 DOCUMENTED SAFETY ANALYSIS TEAM .....	4-2
4.4 ENVIRONMENTAL SAFETY AND HEALTH TEAM.....	4-2
4.5 AUTHORIZATION BASIS SECTION LEADER.....	4-2
5.0 HAZARD ANALYSIS PROCEDURE.....	5-1
5.1 HAZARD IDENTIFICATION .....	5-1
5.1.1 Division of the Facility .....	5-1
5.1.2 Facility Walkdowns .....	5-1
5.1.3 Screening of Standard Industrial Hazards.....	5-2
5.1.4 Results of Hazard Identification .....	5-3

---

## CONTENTS

---

	<u>Page</u>
5.2 HAZARD EVALUATION .....	5-4
5.2.1 Bases for Risk Estimation .....	5-4
5.2.2 Initial Conditions .....	5-5
5.2.3 Scenario Development .....	5-5
5.2.4 Control Identification .....	5-6
5.2.5 Risk Evaluation .....	5-7
5.2.5.1 Unmitigated Risk .....	5-7
5.2.5.2 Mitigated Risk .....	5-9
5.3 HAZARD EVALUATION DSA INPUT .....	5-10
5.3.1 Hazard Evaluation Table .....	5-10
5.3.2 Planned Design and Operational Safety Improvements .....	5-10
5.3.3 Defense in Depth .....	5-11
5.3.4 Worker Safety .....	5-11
5.3.5 Environmental Protection .....	5-11
5.3.6 Accident Selection .....	5-11
6.0 REFERENCES .....	6-1
7.0 TABLES .....	7-1

---

**CONTENTS**

---

Page

APPENDIX A	HAZARD IDENTIFICATION TABLE.....	A-1
APPENDIX B	HAZARDS SCREENING CRITERIA.....	B-1
APPENDIX C	HAZARD EVALUATION TABLE EXAMPLE.....	C-1

---

---

---

**TABLES**


---

	<u>Page</u>
1	Frequency Evaluation Levels ..... 7-2
2	Radiological Consequence Evaluation Levels for Hazard Receptors ..... 7-2
3	Chemical Consequence Evaluation Levels for Hazard Receptors ..... 7-3
4	Risk Binning Matrix — Worker ..... 7-4
5	Risk Binning Matrix — Offsite Public..... 7-5
A-1	Example Hazard Identification Table ..... A-3
B-1	Standard Industrial Hazard Screening Criteria.....B-3
C-1	Frequency Factors Commonly Associated with Controls.....C-3
C-2	Example of Completed Hazard Evaluation Table .....C-4

---

## ACRONYMS

---

AA	Accident Analysis
ANSI	American National Standard Institute
BEU	Beyond Extremely Unlikely
CFR	Code of Federal Regulations
CN	Change Notice
DID	Defense in Depth
DOE	Department of Energy
DOT	Department of Transportation
DSA	Documented Safety Analysis
EG	Evaluation Guideline
ERPG	Emergency Response Planning Guideline
ES&H	Environmental Safety and Health
EU	Extremely Unlikely
FHE	Focused Hazard Evaluation
HA	Hazard Analysis
IC	Initial Condition
LLNL	Lawrence Livermore National Laboratory
NEC	National Electrical Code
NFPA	National Fire Protection Association
OSHA	Occupational Safety and Health Administration
PC	Performance Category
QA	Quality Assurance
RQ	Reportable Quantity
SAR	Safety Analysis Report
SIH	Standard Industrial Hazard
SSC	Structures, Systems, and Component
TEEL	Temporary Emergency Exposure Limit
TLV	Threshold Limit Value
TPQ	Threshold Planning Quantity
TQ	Threshold Quantity
TSR	Technical Safety Requirement

---

This page intentionally left blank.

## **1.0 PURPOSE**

This procedure provides the requirements, responsibilities, and methodology for performing Hazard Analyses (HAs) for Lawrence Livermore National Laboratory (LLNL) Nuclear Hazard Category 2 and 3 Facilities. HAs define the complete spectrum of hazardous events — in terms of hazard identification, potential accident scenarios, and available controls — covered by Documented Safety Analyses (DSAs) and their associated Technical Safety Requirements (TSRs).

This page intentionally left blank.

## 2.0 SCOPE

The scope of this procedure is consistent with HA guidance provided in Chapter 3 of Department of Energy Standard 3009-94, Change Notice Number 1 (DOE-STD-3009-94,CN1) (Ref. 1). This procedure applies to HAs, initiated or revised, after this procedure becomes effective. Additionally, the methodology presented in this procedure meets the HA requirements of 10 Code of Federal Regulations 830 (10 CFR 830) and the LLNL Safety Basis Program Plan for Category 2 and 3 Nuclear Facilities (Ref. 2, 3).

The procedure is applicable to all HAs for LLNL Hazard Category 2 and 3 Nuclear Facilities. Deviations from this procedure require the approval of the Authorization Basis Section Leader. Subcontractors may follow their own HA procedure, provided it meets the requirements of DOE-STD-3009-94 and documentation of the procedure is provided to the Authorization Basis Section Leader and Nuclear Facility Associate Director for review and acceptance prior to beginning the HA.

10 CFR 830 allows nuclear facilities that either have a limited operational life or are subject to deactivation to make use of the alternate safe harbor methodology in DOE-STD-3011-94 (Ref. 4). In that the hazard analysis activities in DOE-STD-3009-94 and DOE-STD-3011-94 are conceptually similar, such DSAs prepared in accordance with either standard will use this procedure or a compliant subcontractor procedure to generate HAs. However, documentation in the resulting DSA may vary from the formal DOE-STD-3009-94 requirements presented in Section 5.3 of this procedure. The minimum documentation required in such cases is specified in DOE-STD-3011-94. This minimum documentation includes the allowance to incorporate existing HAs to the extent practical.

## 2.1 INPUTS

Input to the HA includes the following:

- Facility description
- Process and activity descriptions

## 2.2 OUTPUTS

The primary outputs of the HA include the following:

- Hazard Identification Tables — Comprehensive lists of hazards associated with each facility area. (See Section 5.1, Hazard Identification.)
- Hazard Evaluation Tables — Event descriptions, locations, hazard sources, causes, frequencies, consequences, preventive and mitigative features, and risk binning results for each event. (See Section 5.2, Hazard Evaluation.)

- Explanation of Hazard Evaluation Results — Presented in five DSA subsections: (1) planned design and operational improvements, (2) defense in depth, (3) worker safety, (4) environmental protection, and (5) accident selection. (See Section 5.3, Hazard Evaluation DSA Input.)

### 3.0 TERMS AND DEFINITIONS

**Accident** – An unplanned sequence of events that results in undesirable consequences.

**Accident Analysis**– Those bounding analyses selected for inclusion in the Documented Safety Analysis (DSA). Historically, AA has consisted of the formal development of numerical estimates of the expected consequence and probability of potential accidents associated with a facility. An AA is a follow-on effort to the HA, not a fundamentally new examination requiring extensive original work. As such, it requires documentation of the basis for assignment to a given likelihood of occurrence range in the HA and performance of a formally documented consequence analysis. Consequences are compared with offsite Evaluation Guidelines to identify Safety-Class Structures, Systems, and Components (SSCs).

**Consequence** – The result or effect of a release of hazardous material (radiological, chemical, or biological).

**Defense in Depth** – The DID philosophy is a fundamental approach to hazard control in which no one layer of protection by itself, no matter how good, is solely relied upon. To compensate for potential human and mechanical failures, DID is based on several layers of protection with successive barriers to prevent or mitigate the release of hazardous material to the environment. In keeping with the graded-approach concept, there is no requirement to demonstrate a generic, minimum number of DID layers. However, defining DID as it exists at a given facility is crucial for determining a safety basis. (For a more detailed definition, see DOE-STD-3009-94.)

**Event** – An unplanned occurrence, sequence of occurrences, or phenomena that may result in a release of hazardous material (e.g., radiological, chemical) or energy.

**Facility Area** – A portion of a facility, selected to facilitate hazard identification and evaluation. Areas may be defined by any combination of individual unit operations, individual or grouped facility systems, specific functions, or physical boundaries inside the facility. Facility areas may be the same as facility segments. Guidance on segmentation is given in DOE-STD-1027-92, Change Notice Number 1 (Ref. 5).

**Hazard** – A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel; damage to a facility; or damage to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation).

**Hazard Analysis** – A comprehensive assessment of facility hazards and associated accident scenarios that could produce undesirable consequences for the onsite population, the public, or the environment. Included in the analysis are hazard identification and hazard evaluation.

**Hazard Evaluation** – The step in hazard analysis that evaluates the significance of hazardous situations associated with a process or activity. Hazard evaluations prepared in compliance with this procedure perform both unmitigated and mitigated evaluations, defined as follows:

**Unmitigated Evaluation** – Estimates the risks involved with a facility and its associated operations without regard for safety controls or programs. “Unmitigated” refers to estimating frequency and consequences without taking into account preventive or mitigative features other than initial conditions and the basic physical realities of a given operation.

**Mitigated Evaluation** – Estimates the risks involved with a facility and its associated operations presuming the availability of safety controls and programs.

**Hazard Identification** – A step in hazard analysis that pinpoints material, system, and process/activity characteristics that can produce undesirable consequences.

**Initial Conditions**– Specific assumptions regarding a facility and its operations that are included in unmitigated evaluation. ICs are generally intended to facilitate scenario definition and include items such as inventory information and capabilities of passive features (i.e., no mechanical or human involvement).

**Mitigate** – To lessen the severity of the consequences of an event.

**Offsite Public** – All individuals outside of the DOE site boundary. For LLNL Site 200, this boundary is defined by the perimeter fence line.

**Prevent** – To reduce the frequency of occurrence of an event.

**Risk Binning** – The process of categorizing the relative risk of events by assigning the events a “bin” number from a frequency-consequence matrix (see Section 5.2.2.5, Risk Evaluation). Risk binning is used as an aid in selecting accidents for further evaluation. It is also part of implementing the graded-approach concept.

**Standard Industrial Hazards** – Hazard sources (material or energy) routinely encountered by the general public, or in general industry and construction for which national consensus codes and/or standards exist to govern handling or use without the need for special analysis to define safety design and/or operational parameters.

**Workers** – Individuals either immediately adjacent to or within the occupied area of hazard, or outside the occupied area of hazard but within the site boundary. This latter group is sometimes referred to as co-located workers. In accident analysis, doses are sometimes reported for a generic co-located worker 100 meters from the facility in question.

## **4.0 RESPONSIBILITIES**

The HA is prepared as input to the DSA and, as such, is a part of the DSA process. Responsibilities for those associated with the HA are linked to their responsibilities for developing the DSA. The individual who executes each specific responsibility depends on the facility involved and the level of staffing associated with the HA process. This section specifies responsibilities for various aspects of HA preparation.

### **4.1 FACILITY MANAGER**

The Facility Manager is responsible for the following:

- Authorizing the preparation of a DSA
- Designating the DSA Leader
- Determining the funding and schedule for HA and DSA development
- Identifying the staff to provide facility-specific input to the HA
- Resolving issues and questions regarding facility operations, facility engineering, and regulatory matters
- Approving any calculations associated with the HA
- Ensuring that the HA is documented, either independently or in the DSA, consistent with applicable Quality Assurance (QA) requirements
- Approving the DSA (and the HA included or referenced within it)

### **4.2 DOCUMENTED SAFETY ANALYSIS LEADER**

The DSA Leader is responsible for the following:

- Ensuring that the DSA is developed on schedule and within budget
- Interfacing with facility personnel to ensure that facility-specific inputs to the HA are accurate and consistent with other DSA input
- Working to resolve issues and questions related to the DSA and HA
- Raising issues and questions to the Facility Manager for resolution
- Ensuring that the HA, as part of DSA, is documented and submitted to the Facility Manager, consistent with applicable QA requirements
- Establishing a record file for any generated information that is not specifically incorporated into the DSA

- Ensuring that HA performance involves:
  - qualified staff and appropriate expertise
  - a work plan that includes such information as sources of input, resources, schedule, level of detail, and expected output
  - requests for input, as appropriate, to the Environmental Safety and Health (ES&H) Team
  - assignment and tracking of HA action items
  - documentation of critical assumptions and limitations
  - adequate peer reviewer for technical accuracy

#### **4.3 DOCUMENTED SAFETY ANALYSIS TEAM**

DSA Team members (e.g., operations, criticality safety) are responsible for the following:

- Interacting with facility staff and others to ensure appropriate input to the HA
- Performing their work in accordance with this and other relevant procedures
- Working to resolve issues associated with the HA
- Informing the DSA Leader of issues that may affect the conclusions, budget, or schedule of the HA
- Preparing, documenting, signing, and submitting the HA consistent with applicable QA requirements

#### **4.4 ENVIRONMENTAL SAFETY AND HEALTH TEAM**

The ES&H Team assigned to the facility is responsible for the following (as applicable and when requested):

- Providing input to the HA
- Providing staff with expertise to assist with the HA
- Providing review of HA input and output

#### **4.5 AUTHORIZATION BASIS SECTION LEADER**

The Authorization Basis Section Leader is responsible for the following:

- Approving any deviations from this procedure

- Providing institutional review of the HA, as it is documented in the DSA, against the specifications of this procedure
- Providing staff with expertise to serve as DSA team members when requested.

## **5.0 HAZARD ANALYSIS**

The HA provides a comprehensive assessment of facility hazards that could produce undesirable consequences for LLNL workers and the public. This information is the core data upon which downstream activities such as accident analysis, control selection, and emergency preparedness efforts are based.

Basically, an HA consists of hazard identification followed by hazard evaluation. This includes screening for standard industrial hazards (SIHs), developing hazard-evaluation-table content, and risk-binning scenarios. In addition, the methodology in DOE-STD-3009-94 requires the development of a specific set of topical assessments based on the HA (e.g., DID, worker safety, accident selection).

### **5.1 HAZARD IDENTIFICATION**

Hazard identification is a comprehensive, systematic process by which all known facility hazards (hazardous materials and energy) are identified, recorded, and screened. Screening is performed to eliminate material/energy types and quantities that are considered SIHs, provided those SIHs are not initiators and/or contributors to undesired events that could cause radiological or chemical releases.

The hazard identification process consists of three steps: (1) dividing the facility into “facility areas,” (2) conducting facility walkdowns, and (3) screening for SIHs.

#### **5.1.1 DIVISION OF THE FACILITY**

To facilitate hazard identification and evaluation, the DSA team typically divides a facility into “areas.” These areas may be defined by any combination of individual unit operations, individual or grouped facility systems, specific functions, or physical boundaries inside the facility. The purpose of this subdivision is to organize the hazard analysis effort at its beginning.

Note: The term “facility area” is used in the HA process to distinguish it from “facility segments,” which may have been defined previously during Facility Hazard Classification (per DOE-STD-1027-92). However, this distinction does not preclude the use of facility segments as facility areas.

#### **5.1.2 FACILITY WALKDOWNS**

Facility walkdowns include both physical walkdowns and informational walkdowns. Physical walkdowns permit team members to familiarize themselves first-hand with actual facility systems, processes, practices, equipment, and inventory. Informational walkdowns provide detailed information as team members review existing safety documentation, design/system

drawings, and procedures in the context of hazard identification. The team will perform physical and informational walkdowns to identify hazardous materials and energy sources for each facility area.

An informational walkdown should include a review of the following:

- Facility description (including available drawings)
- Inventory (including information from ChemTrack, Rad Material Balance Area data, hazardous materials lists, and other sources)
- Existing safety documentation (e.g., SARs, Bases for Interim Operation, TSRs, Project Design Documents, Fire Hazards Analyses)
- Facility or Operational Safety Plans
- Consultations with system/process experts, operations staff, ES&H Team, and workers
- Facility occurrence reports
- HAs of neighboring facilities, to determine if an event at one of these facilities could initiate an event at the subject facility

A hazard identification checklist is useful when performing physical or paper walkdowns. Appendix A provides an example checklist. Use of this checklist is recommended, but not required. The checklist has four columns:

- Item — A number or other identifier for each facility hazard.
- Hazard Energy Source or Material — A list of potential hazards that may be in the facility. A long, general list is provided so it can be used for a variety of facilities.
- Exists — To document whether or not the hazard exists in the particular facility area. Each item on the list requires either a “Yes” or a “No” response.
- Description — To describe the hazard in sufficient detail that the DSA Team and reviewers will understand the hazard. The minimum information required for each hazard is type, location (in enough detail to locate the hazard within the facility area), form, and maximum allowable quantity. Other clarifying information (e.g., special storage conditions, nature of toxicity, and by-product hazards such as hydrogen generation by metal dissolution) is also useful to include.

Note: The example checklist is not intended to provide an exhaustive list of potential hazards. It may need to be modified to support the analysis of a given facility.

### 5.1.3 SCREENING FOR STANDARD INDUSTRIAL HAZARDS

The third step in the Hazard Identification process is an initial screening for SIHs. The intent is to keep the DSA evaluation focused on hazardous materials or energy sources and the activities

required to process or handle them. Clarity can be lost through undue emphasis on everyday hazards common in industry, or by focusing on each individual hazard of small-scale activities (e.g., the handling of laboratory quantities of chemicals). In accordance with DOE-STD-3009-94, SIHs are evaluated only to the extent that they could act as initiators and contributors to events that result in a radiological or chemical release. The DSA team screens each identified hazard for each facility area based on material/ energy types and quantities, using the guidance and screening criteria provided in Appendix B.

If an identified hazard meets the appropriate screening criteria, it is deemed to be a SIH, and no further consideration is given to the hazard other than as a potential initiator or contributor to an event that could release radiological or other hazardous material. If the identified hazard does not meet the SIH screening criteria, it is carried forward for hazard evaluation (Section 5.2, Hazard Evaluation). During that process, the hazard or sub-hazard still may be determined to be a SIH and not receive further consideration for designation as a safety SSC or a specific TSR commitment. However, in that case, a formal identification of controls to support that judgment is deemed appropriate. For example, if an X-ray machine passes through the screening criteria of Appendix B, its operation is evaluated. The possibility of worker electrocution may be evaluated for the given configuration, but would not normally be expected to receive safety SSC designation. That aspect of the X-ray machine's hazards would be a SIH and would fall under the appropriate industrial/occupational safety program.

For completeness, all hazard sources screened to be SIHs — and the basis for that determination — must be documented in the hazard identification checklist so they can be considered in terms of their potential for contributing to a material release scenario. Such documentation also assists the Unreviewed Safety Question process by providing a complete list of hazards. That list includes screened hazards that can be used for comparison to see if new hazards have been added or if a hazard no longer meets the SIH screening criteria.

#### 5.1.4 RESULTS OF HAZARD IDENTIFICATION

The raw information collected is distilled into a summary presentation identifying hazards by type, form, location, and maximum allowable quantity. Typically, this is done by developing a table or tables to include in the body of the DSA. Such tables may take whatever form the analyst deems most effective.

DOE-STD-3009-94 specifically requests, at a minimum, that hazards be identified by type, form, location, and quantity. However, for larger nuclear facilities that have many gloveboxes and/or storage locations, it may be impractical to attempt such detailed specification for every potential location. This is particularly true for R&D operations, as opposed to process lines governed by well-defined flow-sheet parameters. Accordingly, bounding surrogate type, form, and quantities may be specified for a given area, operation, or room, reserving detailed accounting by potential location for true process lines. In this case, the standard for adequacy would be whether or not an independent reviewer could derive the material at risk for potential accidents.

The hazard identification presented in the DSA provides the base data for subsequent hazard evaluation and accident analysis (if required). There should be no discrepancies between the information in the hazard identification tables and (1) the types of processes/activities described in Chapter 2 of the DSA (Facility Description) or (2) the information used in downstream analyses.

## 5.2 HAZARD EVALUATION

Hazard evaluation develops the hazards identified into a comprehensive collection of hazardous events, or scenarios. The purpose of the hazard evaluation is to ensure a comprehensive assessment of facility hazards and to provide a largely qualitative risk perspective to help in decision-making for risk reduction.

The hazard evaluation process is divided into six steps: (1) establish bases for risk estimation, (2) identify initial conditions, 3) develop scenarios, (4) identify controls (5) evaluate unmitigated risk, and (6) evaluate mitigated risk. Scenario development, control identification, and risk evaluation typically are performed together on a scenario-by-scenario basis.

The scope of the hazard evaluation includes:

- All facility processes and activities for which DOE authorization is sought
- Natural phenomena (e.g., earthquakes, tornadoes, straight-winds), external events (e.g., aircraft and vehicular impact), and nuclear criticality (where applicable)
- Consideration of the entire spectrum of possible events for a given hazard, in terms of both frequency and consequence (e.g., from a small, localized fire to a large, propagated or facility-wide fire)

The scope of the hazard evaluation does not include:

- Hazards screened to be SIHs
- Willful acts (e.g., sabotage)

Key members of the DSA Team (such as hazard and accident analysts) should be involved in all aspects of the hazard evaluation. Operations and engineering personnel should be consulted when examining their respective areas of interest as well. Specialists (e.g., criticality safety engineers, fire protection engineers, industrial hygienists) should be identified to provide support as needed.

### 5.2.1 BASES FOR RISK ESTIMATION

The hazard evaluation is intended to be a largely qualitative exercise. However, for other than trivial hazards, some basic consequence and frequency indicators are needed to provide

reasonable consistency in the estimation of risk. Therefore, hazard analysis preparers must have a set of basic estimation rules prior to performing the hazard evaluation.

Simple consequence estimates are adequate for this purpose. For radionuclides, the estimation rule could consist of a ground-level dispersion calculation using conservative meteorology (e.g., F stability and 1 m/sec windspeed). Estimating the maximally exposed offsite individual (MOI) dose for the release of 1 gram/1 curie of material provides a ratio that can be scaled easily for differing magnitudes of release. Similar indicators can be calculated for chemicals of major concern.

Frequency estimation in hazard evaluation often involves simple rules of thumb. Table C-1 in Appendix C provides a list of commonly assumed factors for assessing the conditional probability of overall event sequences, whether in mitigated evaluation or in assessing the impact of ICs. That is, a given control type yields an associated frequency reduction for the event resulting from application of that control.

Other estimation inputs might include existing analyses for a given facility, comparable analyses for other facilities, historical data, and expert opinion. Note, however, that when using multiple sources of information it is important that they be integrated into a common framework. If not, inconsistencies can occur in the evaluation process.

### 5.2.2 INITIAL CONDITIONS

The next step prior to actually beginning the evaluation is to determine and document any initial conditions of the evaluation. ICs are specific assumptions that predefine aspects of an operation or activity, such as inventory information or the capabilities of passive features. Some specific examples include:

- A building can withstand specific tornado/high wind, seismic events (e.g., PC-2, PC-3) or specific impacts (e.g., from a small airplane crash)
- Solid transuranic waste is contained in a DOT Type-A drum
- Facility and process inventories are limited to those identified. (Note: The inventory should give specifics such as design information relating to tank volumes and concentrations and location within the facility)
- Inventory form is limited to a specific type resistant to release phenomena
- A specific liquid storage tank is geometrically safe for criticality concerns

It is important to define ICs carefully. Unacknowledged ICs can inappropriately skew both the risk ranking and control selection processes. For example, consider the case of a given material type that is resistant to thermal stress. Presuming that IC, the unmitigated risk of a thermal release is low. If, however, the consequences of a thermal release are significant, the IC represents an important control that must be maintained so that other more vulnerable forms are

not brought into the facility without additional assessment. ICs must be clearly identified so that their significance can be individually evaluated in the control selection process.

### 5.2.3 SCENARIO DEVELOPMENT

Joining a given hazard to an initiating event, or cause, creates one or more possible outcomes. It is also possible for several different initiating events to result in the same outcome. The combination of initiating event and outcome defines a scenario to demonstrate a comprehensive assessment of facility hazards, each of these scenarios should be clearly documented. The minimum information required for a scenario is as follows:

- Scenario-specific designator
- Hazard(s) involved
- Location
- Cause
- Postulated-event description

Designators often include an alphanumeric indicator for accident category (e.g., spill, fire, explosion, earthquake, criticality) to assist in subsequent sorting. This information also can be specified as a separate designation. Hazard and location are specific to the activity or process being evaluated. Cause defines the scenario's initiating event, while the description of the postulated event clearly defines the nature of the scenario in terms of release or other consequence mechanisms.

Scenarios must be developed for every hazard identified in the hazard identification table(s) (Section 5.1.4.). Comparing hazard evaluation entries to the hazard identification table(s) is an effective way to assess completeness. For clarity, separate initiators can be identified as separate events if they do not involve the same set of controls and associated risk considerations. However, the scenarios listed must cover the entire spectrum of possible events for a given hazard — from small-consequence events, for which procedures or equipment are acknowledged to provide adequate protection, to reasonable worst-case conditions.

Note: "Reasonable worst-case" does not require every scenario parameter to be in the most unfavorable state imaginable. For example, if a toxic material is processed as a liquid at room temperature, and no SSC failure can produce uncontrolled heating, a reasonable worst-case condition does not consider a spill with the liquid at its flash point. Likewise, if a given quantity of material would not be assembled into a given configuration for maximum release vulnerability, that theoretical condition need not be assumed. Failure to consider such unrealistic conditions does not require definition of an IC. This distinction is what is meant by the phrase "basic physical realities of a given operation" in the definition of "unmitigated evaluation." It is also consistent with the intent of DOE-STD-3009-94, which states that "facilities should be analyzed as they exist when quantifying meaningful release mechanisms."

#### 5.2.4 CONTROL IDENTIFICATION

For each scenario listed, a complete identification of available safety controls must be provided. This specification includes both: (1) engineered features, in the form of structures, systems, and components and (2) administrative features in the form of specific procedural items (e.g., item is swiped for contamination before being handled) and overall safety management programs. These two types of controls should be identified distinctly.

Either type of control may be further classified as preventive or mitigative. Preventive controls are those that reduce frequency of occurrence. Mitigative controls are those that reduce consequence. Note, however, that these definitions can sometimes overlap depending on the specifics of a scenario. For instance, a combustible loading control program can be considered preventive to the degree it minimizes the opportunity for an isolated initiator to develop into an actual fire. That same program can also be considered mitigative to the degree it prevents a growing fire from spreading to other areas containing additional hazardous material. In such cases, exacting accuracy in classifying the control is not required. A convention should simply be decided upon and implemented consistently. Alternatively in such cases, the control can be listed as both preventive and mitigative.

Engineered features also may be further classified as passive or active. Active controls are those that rely on detection of a hazardous event and/or actuation of the control function. Passive controls provide their function inherently. An example of an active feature would be a fire suppression system that relies on receiving parameter signals to initiate water flow and can thus fail to provide that function in the event of component error. A truly passive feature (e.g., a blast wall) provides a given level of protection constantly. This distinction is relevant in unmitigated risk estimation, where active features are not considered but passive features can be ICs.

#### 5.2.5 RISK EVALUATION

DOE-STD-3009-94 requires some type of risk-ranking mechanism for scenarios. This procedure establishes two four-by-four risk-binning matrices — one for the public and one for workers (see Tables 1 through 5, Section 7.0). Table 1 defines four frequency levels: (1) anticipated, (2) unlikely, (3) extremely unlikely, and (4) beyond extremely unlikely. Tables 2 and 3 define four consequence levels for the public and workers for radiological and chemical exposures: (1) high, (2) moderate, (3) low, and (4) negligible. Since worker consequences in Tables 2 and 3 are defined in qualitative terms, a brief characterization of the effect threshold is provided as well.

The resulting risk matrices for workers and the public are presented in Tables 4 and 5, respectively. The two darker shaded areas on Tables 4 and 5 define high and moderate risk, specified as risk level I and risk level II, respectively. The most lightly shaded and unshaded areas define low and negligible risk, specified as risk level III and risk level IV, respectively. It is useful in evaluating scenarios to record any notes or recommendations made in the process (e.g., unique bases for consequence or frequency estimates, questions to resolve, uncertainties

about facility configuration). Without such a record, the thought process underpinning evaluation results can be lost, causing confusion in review.

The use of these risk matrices in safety SSC and TSR designation is detailed in the LLNL Control Item Selection procedure (AB-007) (Ref. 6).

#### 5.2.5.1 Unmitigated Risk

The initial risk ranking assigned is unmitigated. That is, it reflects the uncontrolled hazard potential of the facility/operation.

Unmitigated frequency does not take into account any active controls or any passive controls not designated as ICs. It is the scenario initiator frequency, as modified by any ICs and consideration of basic physical reality. For example, structural strength is a typical IC factored into the likelihood assigned for specific damage to cause or exacerbate a hazardous material release. Likewise, consideration of basic physical reality would weigh against assuming the likelihood of a flashover fire is simply the initiator frequency (e.g., electrical spark) for an empty concrete storage bay. It would also support not assigning a frequency of “Anticipated” for criticality accidents if the physical properties of a given configuration, such as transuranic waste storage in a drum array, make criticality difficult to achieve even without controls. Allowance for such considerations in frequency can be made when accident selection is primarily based on consequence, as is the case with the frequency-independent Evaluation Guideline specified in Appendix A of DOE-STD-3009-94. Analysts must be careful, however, to avoid the introduction of unacknowledged ICs.

Determining unmitigated consequences is crucial to the entire process laid out in DOE-STD-3009-94 because that process, particularly accident and control selection, is fundamentally consequence-driven. Unmitigated consequences are those estimated without taking into account:

- Active safety features

Example: An interlock that closes a hydrogen supply valve is an active feature that cannot be assumed to eliminate the consequence of an explosion.

- Leakpath reductions in source term

Example: For airborne plutonium particulates, a leakpath factor of unity is assumed even if gravitational settling or HEPA filtration will reduce the quantity released.

Passive features may be assumed in assessing unmitigated consequences provided they meet one of the following three criteria:

- (1) The feature is designated as an IC

Example: See Section 5.2.2.

(2) The feature is necessary to make a release parameter physically meaningful

Example: If material is handled at an elevation of three feet, the unmitigated evaluation does not require assuming drop heights greater than that. Appendix A of DOE-STD-3009-94 provides the further example of a can containing material of concern. It states that if the can is dropped, the material should not be assumed to fall in an uncontained manner.

(3) The feature is substantially unaffected by the accident scenario

Example: If a given hazardous-material collection tank is not damaged by a postulated explosion in a room, the unmitigated evaluation does not assume release of that material.

Note: The third criterion does not apply to SSCs specifically engineered for an accident, such as a blast shield that protects personnel from an explosion. If assumed, such SSCs should be considered ICs.

ICs must be individually evaluated for safety SSC and TSR designation. Unaffected features, or features necessary for physically meaningful definition, are not ICs and do not automatically require consideration for safety SSC and TSR designation. The LLNL Control Item Selection procedure (AB-007) provides additional guidance on this subject.

When estimating consequence or frequency, it is best to err in the conservative direction. For example, a frequency of occurrence roughly estimated as  $9 \times 10^{-3}/\text{yr}$  would be on the high end of the “unlikely” frequency range. The DSA Team, considering the sources, methods, and uncertainties associated with this value, might collectively decide to bin the event in the “anticipated” frequency range.

#### 5.2.5.2 Mitigated Risk

After determining unmitigated risk, an assessment is made of mitigated risk. This provides analytical assurance that the hazard potential of a given facility/operation is adequately controlled. Together, the unmitigated and mitigated evaluations constitute the risk perspective needed for LLNL and DOE decision-making.

Mitigated risk is expected to have lower frequency, lower consequence, or both relative to unmitigated risk. In general, there should be sufficient controls that scenarios with an unmitigated risk rank of I or II will have a mitigated risk rank of III or IV. Where this is not the case, specific justification must be provided as to why additional controls are not feasible. Mitigated risk evaluation is also performed for scenarios with an unmitigated risk rank of III, but no specific

reduction is required. No mitigated risk evaluation is required for events assigned an unmitigated risk rank of IV.

To assist in identifying control flowdown to safety SSC and TSR designation, those controls that reduce risk rank I or II scenarios to rank III or IV must be identified in some manner. This can be accomplished by specific notation or by using a signifier such as an asterisk, bold notation, or underlining. Such identification does not require subsequent designation as a safety SSC; it only indicates a candidate for such designation.

There is one exception to the preceding paragraph. The safety significant designation process for worker safety is not expected to include controls associated with standard industrial hazards, even if those hazards exceed the screening criteria in Appendix B. For example, liquid nitrogen dewars, a common feature in labs, can represent an asphyxiation hazard in unmitigated assessment. Identifying how that hazard is controlled is perfectly appropriate. Yet, it represents a common enough hazard, with sufficiently well defined precedents for handling, that designation as safety equipment of special significance is unwarranted. Accordingly, a bold notation of “SIH” may be used in lieu of specific control parsing.

Note: If there is too much uncertainty in evaluating mitigated results, the analyst may defer the mitigated risk evaluation until after the accident analysis. This option is left to the discretion of the analyst. In any event, the HA and the AA, when developed, should always be checked against one another to ensure consistency.

### **5.3 HAZARD EVALUATION DSA INPUT**

DOE-STD-3009-94 requires an organized summary of HA results, as opposed to simply presenting the raw results by themselves. This summary defines the facility and its principal safety issues upon which the DOE and the facility operator must agree.

#### **5.3.1 HAZARD EVALUATION TABLE**

The hazard evaluation table included or referenced in the DSA may be developed either during or after the HA, depending on whether it is felt necessary to reorganize the accumulated information into a more presentable format. Post-production is an allowed option because hazard evaluations can generate a great deal of information, some of which initially may be captured in short hand.

There is no one correct format for a DSA hazard evaluation table. The example provided in Appendix C is not intended as a requirement. The only requirement is to capture, in an easily understood form, the following information:

- Event designator
- Hazard(s) involved
- Location

- Postulated-event description
- Causes/Initiators
- Controls (specifically called out as SSCs or administrative, and preventive or mitigative)
- Risk ranking (both unmitigated and mitigated)

As noted previously, it also can be useful to include a column for notes and recommendations. This can be helpful to both preparer and reviewer in any subsequent review process. The amount of information specified above, however, can result in a table cramped for space. If so, risk ranking and the specific control citations associated with that ranking can be split off into a second table. If this is done, care should be taken to maintain continuity of event designators so as to avoid confusion.

### 5.3.2 PLANNED DESIGN AND OPERATIONAL SAFETY IMPROVEMENTS

This information is requested in Section 3.3.2.3.1 of DOE-STD-3009-94. Two types of entries typically are provided. The first type consists of commitments to improvements not yet implemented, with proposal of any interim controls deemed necessary. Such commitments are made when it is not considered feasible to implement the design or operational improvements prior to DSA submittal.

The second type consists of identified improvements to operations made as a result of the HA. This type of entry is not required. However, it can, be useful in demonstrating the thoroughness of the HA process to DOE.

### 5.3.3 DEFENSE IN DEPTH

This information is requested in Section 3.3.2.3.2 of DOE-STD-3009-94. DID defines those aspects of design and operation, including safety management programs, that prevent a major uncontrolled release of hazardous material or energy, independent of receptor. It is, in effect, the overall definition of why the facility is considered safe.

DOE-STD-3009-94 discusses this definition in terms of: (1) systematic organization of discussion, starting with hazardous material or energy and working outward, (2) focus on the functional big picture, as opposed to detailed design specifics, (3) correlation of individual functions to layers of defense, and (4) a summation of why the DID described satisfies general practice for the type of hazards being evaluated. A rule of thumb for evaluating DID adequacy is to consider whether or not a technical reviewer not familiar in detail with a facility's operation could understand the facility's principle hazards and controls based on reading this section alone.

After completing the HA, analysts should have a clear concept of the desired facility safety basis. That concept must be clearly and completely articulated in this section. Preparers should

not presume that reviewers will arrive at the same concept from information scattered across multiple sections of the DSA.

#### 5.3.4 WORKER SAFETY

This information is requested in Section 3.3.2.3.3 of DOE-STD-3009-94. It is intended to explain any major aspects of worker protection not already covered by DID.

#### 5.3.5 ENVIRONMENTAL PROTECTION

This information is requested in Section 3.3.2.3.4 of DOE-STD-3009-94. It is intended to explain any major aspects of environmental protection not already covered by DID.

#### 5.3.6 ACCIDENT SELECTION

This information is requested in Section 3.3.2.3.5 of DOE-STD-3009-94. It is intended to explain why only a small number of accidents, from all the scenarios listed in the hazard evaluation, are selected for documentation in the accident analysis. The three main bases for accident selection are: (1) accident type, (2) potential consequence; and (3) associated controls.

DOE-STD-3009-94 states that at least one bounding accident from each of the major types determined from the hazard analysis (e.g., fire, explosion, spill, seismic, etc.) should be selected for accident analysis unless the associated public consequences are clearly minimal. These accidents are called representative accidents. The minimum expectation for accident selection is to identify a complete set of representative accidents.

Accident analysis is performed to formally document estimated accident consequences and to compare those consequences against Evaluation Guidelines (EGs). The EG in Appendix A of DOE-STD-3009-94 (i.e., 25 rem to a hypothetical maximally exposed offsite individual) is defined for the public. Therefore, accident selection is based on public consequences. Accident selection should not be based on the risk bins assigned in Section 5.2.5, “Risk Evaluation,” in place of actual consequence. That is, the bounding consequence event for a given type of accident must be selected for accident analysis irrespective of whether it is assigned a lower unmitigated frequency bin than a lesser consequence event, which may actually represent the higher risk. To select by risk bin would allow dismissal of events potentially challenging the EG in favor of those that do not, which is inconsistent with DOE guidance. This stipulation does not, however, preclude likelihood issues from influencing the basic event definition (e.g., duration and intensity of a fire), consistent with the discussion in Section 5.2.3, “Scenario Development,” regarding “reasonable worst case” scenarios as opposed to every circumstance in the most unfavorable condition imaginable.

Finally, the purpose of the EG is to determine if safety class SSC designation is required. If two explosions both challenge EGs and involve different controls, both explosions must be selected for accident analysis. Otherwise, controls potentially requiring safety class designation would

not be assessed. Multiple accidents of a given type selected for this reason are called “unique accidents.”

The key features of a clear explanation for accident selection include:

- Selection based on consequence (the 25-rem EG is not risk-based).
- Grouping accidents by type (i.e., representative accidents) for ease of comparison
- Inclusion of at least one representative accident for each major type, unless the consequences are clearly minimal
- Consideration of associated controls (i.e., unique accidents)

Presentation of complex logic models to support accident selection is discouraged, particularly when layered in acronyms and mnemonics. Experience dictates that such derivations obscure clarity and may prolong the review process.

## 6.0 REFERENCES

1. Preparation Guide for U.S. Department of Energy Non-Reactor Nuclear Facility Safety Analysis. DOE-STD-3009-94, Change Notice #1, U.S. Department of Energy, Washington, DC, January 2000.
2. Nuclear Safety Management. 10 CFR Part 830, U.S. Department of Energy, Washington, DC.
3. Safety Basis Program Plan for Hazard Category 2 and 3 Nuclear Facilities. AB-001, Lawrence Livermore National Laboratory, Livermore, CA, August 2001.
4. Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plans. DOE-STD-3011-94, U.S. Department of Energy, Washington, DC, November 1994.
5. Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23. DOE-STD-1027-92, Change Notice #1, U.S. Department of Energy, Washington, DC, September 1997.
6. Control Item Selection Procedure for Hazard Category 2 and 3 Nuclear Facilities. AB-007, Lawrence Livermore National Laboratory, Livermore, CA, 2002.
7. Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities. DOE-STD-1020-02, U.S. Department of Energy, Washington, DC, January 2002.

This page intentionally left blank.

## **7.0 TABLES**

**Table 1: Frequency Evaluation Levels**

Frequency Level	Acronym	Frequency	Qualitative Description
Anticipated	A	$f \geq 10^{-2}$ /yr	Events that might occur several times during the lifetime of the facility (excluding normal operations)
Unlikely	U	$10^{-4} \leq f < 10^{-2}$ /yr	Events not anticipated during the lifetime of the facility
Extremely Unlikely	EU	$10^{-6} \leq f < 10^{-4}$ /yr	Events that will probably not occur during the lifetime of the facility
Beyond Extremely Unlikely	BEU	$f < 10^{-6}$ /yr	All other Events

**Table 2: Radiological Consequence Evaluation Levels for Hazard Receptors**

Consequence Level (Abbreviation) ↓	Offsite Public	Worker
High (H)	$C \geq 25.0$ rem	prompt worker fatality, acute injury that is immediately life threatening or permanently disabling  Rad Exposure = Large prompt dose (e.g., criticality level)
Moderate (M)	$5.0 \leq C < 25.0$ rem	serious injury, no immediate loss of life, no permanent disabilities, hospitalization required  Rad Exposure = for alpha emitters, a very energetic release to an occupied area; essentially a major accident destroying barriers as opposed to a confinement leaks.
Low (L)	$0.1 \leq C < 5.0$ rem	minor injuries, no hospitalization  Rad Exposure = glovebox leak or small-scale confinement failure; typical DOE complex occupational worker contamination or uptake
Negligible (N)	$C < 0.1$ rem	Rad Exposure = Minimal expectation of contamination or uptake

**Table 3: Chemical Consequence Evaluation Levels for Hazard Receptors**

Consequence Level (Abbreviation) ↓	Offsite Public	Worker
High (H)	$C \geq \text{ERPG-3}$	prompt worker fatality, acute injury that is immediately life threatening or permanently disabling  Chem Exposure = Sustained IDLH level, truly life-threatening as opposed to pop up over ERPG-3 for a few minutes; permanent effects may occur.
Moderate (M)	$\text{ERPG-2} \leq C < \text{ERPG-3}$	serious injury, no immediate loss of life, no permanent disabilities, hospitalization required  Chem Exposure = Hospitalized with evident distress; lingering physical effects in hospital, though none permanent.
Low (L)	$\text{ERPG-1} \leq C < \text{ERPG-2}$	minor injuries, no hospitalization  Chem Exposure = Short-term effects that dissipate quickly upon egress (e.g., eyes watering, cough)
Negligible (N)	$C < \text{ERPG-1}$	$C < \text{Low}$  Chem. Exposure = No effects beyond odor

Note: If Emergency Response Planning Guideline (ERPG) does not exist, the Temporary Emergency Exposure Limit (TEEL) should be used. (TEEL-3 = ERPG-3, TEEL-2 = ERPG-2, TEEL-1 = ERPG-1)

For non-radiological or chemical worker hazards, the base qualitative definitions, as written in both tables, should be used for assessment (e.g., death, hospitalization, minor injury).

**Table 4: Risk Binning Matrix — Worker**

Frequency → Consequence ↓	Beyond Extremely Unlikely $f < 10^{-6}$ /yr	Extremely Unlikely $10^{-6} \leq f < 10^{-4}$ /yr	Unlikely $10^{-4} \leq f < 10^{-2}$ /yr	Anticipated $f \geq 10^{-2}$ /yr
<b>High</b>  Prompt worker fatality, acute injury that is immediately life threatening or permanently disabling	<b>III</b>	<b>II</b>	<b>I</b>	<b>I</b>
<b>Moderate</b>  Serious injury, no immediate loss of life, no permanent disabilities, hospitalization required	<b>IV</b>	<b>III</b>	<b>II</b>	<b>I</b>
<b>Low</b>  Minor injuries, no hospitalization	<b>IV</b>	<b>IV</b>	<b>III</b>	<b>III**</b>
<b>Negligible</b>  C < Low	<b>IV</b>	<b>IV</b>	<b>IV</b>	<b>IV</b>

\*\*Shifts to III for worker matrix based on the fact that Low consequences are anticipated events for workers.

**Table 5: Risk Binning Matrix — Offsite Public\***

Frequency → Consequence ↓	Beyond Extremely Unlikely $f < 10^{-6} / \text{yr}$	Extremely Unlikely $10^{-6} \leq f < 10^{-4} / \text{yr}$	Unlikely $10^{-4} \leq f < 10^{-2} / \text{yr}$	Anticipated $f \geq 10^{-2} / \text{yr}$
<b>High</b> <u>Radiological</u> : $C \geq 25$ rem <u>Chemical</u> : $C \geq \text{ERPG-3}$	III	II	I	I
<b>Moderate</b> <u>Radiological</u> : $5 \leq C < 25$ rem <u>Chemical</u> : $\text{ERPG-2} \leq C < \text{ERPG-3}$	IV	III	II	I
<b>Low</b> <u>Radiological</u> : $0.1 \leq C < 5$ rem <u>Chemical</u> : $\text{ERPG-1} \leq C < \text{ERPG-2}$	IV	IV	III	II
<b>Negligible</b> <u>Radiological</u> : $C < 0.1$ rem <u>Chemical</u> : $C < \text{ERPG-1}$	IV	IV	IV	IV

\*Note that accident selection for accident analysis is based on consequence, and is thus not limited to choosing events in the shaded risk bins. The unshaded risk bins are only a means to indicate that risk appears adequately controlled. Any event whose consequences challenge or exceed the 25 rem EG must be evaluated in accident selection, provided the event meets DOE-STD-3009-94 frequency guidelines for inclusion in the DSA to begin with. The LLNL Accident Analysis (AB-005) procedure specifies those guidelines in Section 5.1, “Design Basis Accidents.”

This page intentionally left blank.

**APPENDIX A**

**HAZARD IDENTIFICATION TABLE**

This page intentionally left blank.

**Table A-1: Example Hazard Identification Table**

<b>Item</b>	<b>Hazard Energy Source or Material</b>	<b>Exists (Y/N)</b>	<b>Description</b>
<b>1.0</b>	<b>Electrical</b>		
1.1	Battery banks		
1.2	Cable runs		
1.3	Diesel generators		
1.4	Electrical equipment		
1.5	Heaters		
1.6	High voltage (> 600V)		
1.7	Locomotive, electrical		
1.8	Motors		
1.9	Power tools		
1.10	Pumps		
1.11	Service outlets, fittings		
1.12	Switchgear		
1.13	Transformers		
1.14	Transmission lines		
1.15	Wiring / underground wiring		
1.16	Other		
<b>2.0</b>	<b>Thermal</b>		
2.1	Boilers		
2.2	Bunsen burner / hot plates		
2.3	Electrical equipment		
2.4	Electrical wiring		
2.5	Engine exhaust		
2.6	Furnaces		
2.7	Heaters		
2.8	Lasers		
2.9	Steam lines		
2.10	Welding surfaces		
2.11	Welding torch		
2.12	Other		
<b>3.0</b>	<b>Pyrophoric Material</b>		
3.1	Pu and U metal fines		
3.2	Other		
<b>4.0</b>	<b>Open Flame</b>		
4.1	Bunsen burners		
4.2	Welding / cutting torches		
4.3	Other		
<b>5.0</b>	<b>Flammables</b>		
5.1	Cleaning / decon solvents		
5.2	Flammable gases		
5.3	Flammable liquids		
5.4	Gasoline		

Item	Hazard Energy Source or Material	Exists (Y/N)	Description
5.5	Natural Gas		
5.6	Nitric acid soaked rags (spontaneous combustion)		
5.7	Nitric acid and organics		
5.8	Paint / paint solvent		
5.9	Propane		
5.10	Spray paint		
5.11	Other		
<b>6.0</b>	<b>Combustibles</b>		
6.1	Paper / wood products		
6.2	Petroleum based products		
6.3	Plastics		
6.4	Other		
<b>7.0</b>	<b>Chemical Reactions</b>		
7.1	Concentration		
7.2	Disassociation		
7.3	Exothermic		
7.4	Incompatible chemical mixing		
7.5	Uncontrolled chemical reactions		
<b>8.0</b>	<b>Explosive Material</b>		
8.1	Caps		
8.2	Dusts		
8.3	Dynamite		
8.4	Electric squibs		
8.5	Explosive chemicals		
8.6	Explosive gases		
8.7	Hydrogen		
8.8	Hydrogen (batteries)		
8.9	Nitrates		
8.10	Peroxides		
8.11	Primer cord		
8.12	Propane		
8.13	Other		
<b>9.0</b>	<b>Kinetic (Linear and Rotational)</b>		
9.1	Acceleration / deceleration		
9.2	Bearings		
9.3	Belts		
9.4	Carts / dollies		
9.5	Centrifuges		
9.6	Crane loads (in motion)		
9.7	Drills		
9.8	Fans		
9.9	Firearm discharge		

<b>Item</b>	<b>Hazard Energy Source or Material</b>	<b>Exists (Y/N)</b>	<b>Description</b>
9.10	Fork lifts		
9.11	Gears		
9.12	Grinders		
9.13	Motors		
9.14	Power tools		
9.15	Presses / shears		
9.16	Rail cars		
9.17	Saws		
9.18	Vehicles		
9.19	Vibration		
9.20	Other		
<b>10.0</b>	<b>Potential (Pressure)</b>		
10.1	Autoclaves		
10.2	Boilers		
10.3	Coiled springs		
10.4	Furnaces		
10.5	Gas bottles		
10.6	Gas receivers		
10.7	Pressure vessels		
10.8	Pressurized system (e.g., air)		
10.9	Steam headers and lines		
10.10	Stressed members		
10.11	Other		
<b>11.0</b>	<b>Potential (Height / Mass)</b>		
11.1	Cranes / hoists		
11.2	Elevated doors		
11.3	Elevated work surfaces		
11.4	Elevators		
11.5	Lifts		
11.6	Loading docks		
11.7	Mezzanines		
11.8	Floor pits		
11.9	Scaffolds and ladders		
11.10	Stacked material		
11.11	Stairs		
11.12	Other		
<b>12.0</b>	<b>Internal Flooding Sources</b>		
12.1	Domestic water		
12.2	Fire suppression piping		
12.3	Process water		
12.4	Other		
<b>13.0</b>	<b>Physical</b>		
13.1	Sharp edges or points		

Item	Hazard Energy Source or Material	Exists (Y/N)	Description
13.2	Pinch points		
13.3	Confined space		
13.4	Tripping		
<b>14.0</b>	<b>Radiological Material</b>		
14.1	Radiological material		
<b>15.0</b>	<b>Hazardous Material</b>		
15.1	Asphyxiants		
15.2	Bacteria / viruses		
15.3	Beryllium and compounds		
15.4	Biologicals		
15.5	Carcinogens		
15.6	Chlorine and compounds		
15.7	Corrosives		
15.8	Decontamination solutions		
15.9	Dusts and particles		
15.10	Fluorides		
15.11	Hydrides		
15.12	Lead		
15.13	Oxidizers		
15.14	Poisons (herbicides, insecticides)		
15.15	Other		
<b>16.0</b>	<b>Ionizing Radiation Sources</b>		
16.1	Contamination		
16.2	Electron beams		
16.3	Radioactive material		
16.4	Radioactive sources		
16.5	Radiography equipment		
16.6	X-ray machines		
16.7	Other		
<b>17.0</b>	<b>Non-Ionizing Radiation</b>		
17.1	Lasers		
17.2	Other		
<b>18.0</b>	<b>Criticality</b>		
18.1	Fissile material		
<b>19.0</b>	<b>Non-facility Events</b>		
19.1	Explosion		
19.2	Fire		
19.3	Power outage		
19.4	Other		
<b>20.0</b>	<b>Vehicles in Motion</b>		
20.1	Airplane		
20.2	Crane / hoist		
20.3	Forklifts		

<b>Item</b>	<b>Hazard Energy Source or Material</b>	<b>Exists (Y/N)</b>	<b>Description</b>
20.4	Heavy construction equipment		
20.5	Helicopter		
20.6	Train		
20.7	Truck / car		
<b>21.0</b>	<b>Natural Phenomena</b>		
21.1	Earthquake		
21.2	Flood		
21.3	Lightning		
21.4	Rain / hail		
21.5	Snow / freezing weather		
21.6	Straight wind		
21.7	Tornado		

This page intentionally left blank.

## **APPENDIX B**

### **HAZARD SCREENING CRITERIA**

This page intentionally left blank.

**Table B-1: Hazard Screening Criteria**

<b>Hazard</b>	<b>Criteria/Measure</b>	<b>Guidance</b>
Chemical Hazards	This appendix	Reportable Quantity (RQ), Threshold Quantity (TQ), Threshold Planning Quantity (TPQ) screening values as discussed in this appendix
Toxic Material	This appendix	RQ, TQ, TPQ screening values as discussed in this appendix
X-Ray Equipment	Does not meet American National Standard Institute (ANSI) X-Ray standards	Applicable national codes and standards (e.g., American Nuclear Society (ANS) N537/NBS123)
Flammable Materials	N/A	Considered as a contributor/initiator for fire events.
Reactive Material	N/A	Screened according to RQ, TQ, TPQ screening values per SARA #00-26
Chemical Compatibility	N/A	Screened according to RQ, TQ, TPQ screening values per SARA #00-26
Lasers	Class III non-enclosed beam Class IV	ANSI Z136.1 "Safe Use of Lasers classifies lasers in Classes I through IV"
Electrical	>600 volts or >600 volts and >24 milli-Ampere or >50j stored energy at 600 volts	National Electric Code identifies these as systems requiring special considerations
Kinetic Energy	"Unique or Unusual" high kinetic energy sources (e.g., high energy flywheels, large centrifuges)	Many high kinetic energy systems are capable of causing personnel injury. Most of these (e.g., cars, trucks, forklifts, cranes) are standard industrial hazards unless an initiator for another significant event. Unique systems (e.g., high energy flywheels, large centrifuges) are not considered standard industrial hazards.
Pressure	Stored energy >0.1 LB TNT Pressure > 3000 psig	High hydraulic pressures and pressurized gas bottles are standard industrial hazards. Large volumes of compressed gases are not routine.
Temperature	Temperatures which could act as an initiator	High temperature systems are standard industrial hazards but an evaluation is required if the temperature could result in an overpressure, creation of toxic products or cause a fire.
Biohazards	As identified by HP or Industrial Hygiene	
Asphyxiants	Oxygen content less than 18%	Asphyxiants do not have Threshold Limit Value (TLV) and cannot be handled as toxic material. Consider areas that could entrap asphyxiants and areas storing cylinders of asphyxiants

The criteria in this appendix are provided to facilitate screening of obvious standard industrial hazards (SIHs). Failure to satisfy these criteria does not rule out ultimately identifying a given hazard or sub-hazard as a SIH. It requires that a hazard evaluation assess potential events and associated controls to support such a determination.

## **B.1 CHEMICAL SCREENING CRITERIA**

The lists of chemicals considered to be hazardous are given in 40 CFR 302, 40 CFR 355, 29 CFR 1910.119, and 40 CFR 68.130 (Ref. 1, 2, 3, 4).

A chemical is screened if any of the following conditions apply:

- The chemical is on the referenced lists, but is less than the RQ (40 CFR 302, 40 CFR 355) (Ref. 1, 2).
- The chemical is not on the referenced lists, but satisfies one of the following conditions:
  - Is less than 1 pound of solids or liquids
  - Is less than 100 pounds of solids or liquids, or 10 pounds of gasses, with National Fire Protection Association (NFPA) Health Hazard ratings of 1 or 2 or TEEL-2 greater than 100 ppm
  - Is in common use by office workers, the public, or others

## **B.2 X-RAY EQUIPMENT AND ACCELERATORS**

The intent is to screen out those facilities with X-ray equipment or simple accelerators that are commercially available, conform to appropriate national codes and standards (e.g., ANS N537/NBS123 for X-ray equipment or ANS 43.1 for accelerators), and have not been modified with regard to safety-related design and operating features, such as voltage and shielding. If the X-ray system does not conform to the appropriate national code standard or the accelerator is considered “complex,” it must be identified for further HA. (See Section 2.6.2.3.2 of ANS 43.1, Complex Accelerators, for the definition of simple and complex accelerators.)

## **B.3 LASERS**

The intent is to screen out Class I and II lasers and Class III lasers with enclosed beams (per ANSI Z136.1) because they do not represent a significant health threat. If these Class I, II, and III laser systems do not conform to the appropriate national standard, they must be identified for further HA. Class III lasers with non-enclosed beams and Class IV lasers are to be identified for further analysis. Gas supplies that are an integral part of an unmodified, sealed, purchased system do not have to be treated separately. However, gas supplies that are not sealed in a purchased system or systems that have been modified must be considered separately, as appropriate (i.e., toxic material criteria). Replacing integral gas cylinders is not considered a modification.

## **B.4 ELECTRICAL**

The intent is to screen out standard electrical hazards, but to retain for further analysis those that represent special safety concerns. Systems to be retained are (1) those with 600 volts or more and 25 milli-amperes or more output and (2) stored-energy systems with 50J or more stored energy and terminal-to-terminal voltage of 600 volts or more. The National Electric Code (NEC) 70-1990 identifies these as systems requiring special consideration.

## **B.5 TEMPERATURE**

The intent is to screen out high-temperature systems whose only consequence is a contact burn and to keep for further analysis those systems that could result in a strong overpressure if a coolant or other fluid contacted the high-temperature mass, could cause toxic products if materials in the area were exposed to the high temperature, or could cause a fire that would spread radioactive or toxic materials.

## **B.6 BIOHAZARDS**

The intent is to screen out common sources of biohazards (e.g., cooling towers), but to retain for further, analysis facilities containing biohazards that require special industrial hygiene controls (e.g., protective clothing, breathing apparatus, special warning placards).

## **B.7 ASPHYXIAN**

Asphyxiants do not have TLVs and, therefore, cannot be handled as toxic materials. Consider if there are areas that could entrap asphyxiants and unsuspecting personnel or situations that would impact large numbers of people. Cylinders of compressed asphyxiants should be included in these evaluations. Such situations should be identified for further analysis. Specifically, those situations in which the oxygen level would be less than 18% due to increased asphyxiant gas concentration should be kept for further analysis.

## **B.8 ADDITIONAL GUIDANCE**

The LLNL *Environment, Safety and Health Manual* provides additional guidance on hazard screening (Ref. 5). Additionally, hazardous materials or operations that are encountered in general industry in appropriate applications and that are adequately controlled by OSHA regulations or one or more national consensus standards (e.g., American Society of Mechanical Engineers, ANSI, NFPA, Institute of Electrical and Electronics Engineers, NEC) that adequately define special safety requirements are considered to be SIHs. SIHs must be considered as initiators for accidents involving hazards that are not SIHs. For example, a flammable material may be screened out as a SIH. If, however, the flammable material potentially could cause a fire

that releases toxic or radioactive materials, that material must be considered as a potential initiator for the release.

## **B.9 REFERENCES**

1. “Protection of the Environment,” Title 40 Code of Federal Regulations, Part 302.4, Designation, Reportable Quantities, and Notification. U.S. Environmental Protection Agency, Washington, DC July 1992.
2. “Protection of the Environment,” Title 40 Code of Federal Regulations, Part 355, Emergency Planning and Notification. U.S. Environmental Protection Agency, Washington, DC, July 1992.
3. “Labor,” Title 29 Code of Federal Regulations, Part 1910.119(e)(6), Process Safety Management Of Highly Hazardous Chemicals. U.S. Department of Labor, Washington, DC, May 26, 1992.
4. “Protection of the Environment,” Title 40 Code of Federal Regulations, Part 68, Accidental Release Prevention Requirements: Risk Management Programs Under Clean Air Act. U.S. Environmental Protection Agency, Washington, DC, March 1995.
5. LLNL Environmental, Safety and Health Manual. Lawrence Livermore National Laboratory, Livermore, CA.

## **APPENDIX C**

### **HAZARD EVALUATION TABLE EXAMPLE**

This page intentionally left blank.

**Table C-1: Frequency Factors Commonly Associated with Controls**

Type of Control	Frequency Factor
<b>Engineering Features</b>	
Passive Structural (e.g., Building structural design, permanent shielding)	1E-4 <sup>1,2</sup>
Passive mechanical (e.g., qualified container)	1E-4 <sup>1,2</sup>
Passive electrical (e.g., grounding)	1E-4 <sup>1,2</sup>
Active fail-safe mechanical (e.g., spring loaded valve)	1E-3 <sup>1,2</sup>
Active fail-safe electrical (e.g., fails safe on loss of power)	1E-3 <sup>1,2</sup>
Active mechanical safety related pedigree (e.g., safety related pump)	1E-3 <sup>1,2</sup>
Active electrical safety related pedigree (e.g., safety related UPS)	1E-3 <sup>1,2</sup>
Active mechanical safety related non-pedigree (e.g., industrial like sprinkler)	1E-2 <sup>1,2</sup>
Active electrical safety related non-pedigree (e.g., non-safety related switch)	1E-2 <sup>1,2</sup>
Fail safe detection and alarm systems	1E-3 <sup>1,2</sup>
Non-fail safe detection and alarm systems	1E-2 <sup>1,2</sup>
Certified personnel (e.g., forklift drivers)	1E-2 <sup>3</sup>
Follow written procedures for non-specific safety controls	1E-1 <sup>3</sup>
Nonproceduralized practices	1E-1 <sup>3</sup>
Preventive maintenance of non-safety related equipment	1E-1 <sup>3</sup>
Training with no certification	1E-1 <sup>3</sup>

<sup>1</sup> Source—Component Failure Rate Data with Potential Applicability to Plutonium Facilities, DPST-CFRP-111, E.I. DuPont de Nemours & Co., Savannah River Laboratory, 1980

<sup>2</sup> Source—Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), NUREG/CR-4639, U.S. NRC, December 1980

<sup>3</sup> Source—NUREG/CR-1278—Handbook of Human Reliability with Emphasis on Nuclear Power Plant Applications, A.D. Swain, H.E. Guttman, August 1983